Formularz oceny spełniania obowiązków wynikających z *rozporządzenia ws. ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO)* oraz *ustawy o ochronie danych osobowych (uodo)*

1. *Formularz oceny RODO* został **opracowany przez międzyresortowy zespół roboczy audytorów wewnętrznych i kontrolerów** z Kancelarii Prezesa Rady Ministrów, Ministerstwa Sprawiedliwości, Ministerstwa Rodziny, Pracy i Polityki Społecznej oraz Ministerstwa Finansów. Jest to podsumowanie dotychczasowych doświadczeń ww. jednostek oraz wypracowanych materiałów wewnętrznych w zakresie przygotowania służb audytu i kontroli do realizacji zadań związanych z oceną systemu ochrony danych osobowych (dalej: DO).

2. **Celem opracowania niniejszego formularza jest metodyczne wsparcie służb audytu i kontroli** w jednostkach administracji państwowej. Jest to materiał o charakterze generalnym, dlatego może być wykorzystywany przez wszystkie jednostki administracji (w tym rządowej i samorządowej) jako merytoryczna pomoc w realizacji zadań kontrolnych i audytowych.

3. **Materiał przedstawia najważniejsze zagadnienia, których może dotyczyć ocena**. Prezentowane obszary badania / zagadnienia i pytania kontrolne oraz wskazówki metodyczne **nie są wyczerpujące ani obowiązkowe**, powinny być więc różnicowane i dostosowywane w zależności do rodzaju, charakteru i skali przetwarzania DO w danej jednostce. Mając to na uwadze **zachęcamy Państwa do swobodnego uzupełniania i modyfikowania formularza** zgodnie z własną metodyką działania, przyjętymi celami audytu lub kontroli oraz charakterystyką przetwarzania DO w badanej jednostce.

4. Formularz składa się z 49 obszarów badania (łącznie 111 wymogów), które pogrupowano w **VII rozdziałach skupiających się na kolejnych perspektywach zarządzania systemem ochrony danych osobowych**, tj.:
   - planowaniu i organizacji tego systemu (rozdz. *I. Organizacja systemu ochrony DO, w tym administratorzy, współadministratorzy i podmioty przetwarzające*),
   - zapewnieniu poprawności procesów przetwarzania (rozdz. *II. Prawo do przetwarzania DO* i III. *Realizacja praw osoby, której dane dotyczą*) oraz
   - mechanizmach monitorowania i nadzoru nad tym procesem (rozdz. *IV. Inspektor Ochrony Danych*, *V. Rejestrowanie czynności przetwarzania*, *VI. Ocena skutków przetwarzania DO*, *VII. Naruszenie ochrony DO)*.

5. Konstrukcja formularza wymusza dokonanie **podsumowania i oceny na poziomie zdefiniowanych obszarów**, ale wykorzystanie tych ocen nie jest obowiązkowe. Podobnie zdefiniowana skala ocen (*pozytywna*, *zastrzeżenia*, *negatywna*, *w realizacji*, *nie dotyczy*), również może być stosownie modyfikowana, w zależności od przyjętej metodyki badania (np. *spełnia, częściowo spełnia albo nie spełnia wymogów, uwaga, ryzyko naruszenia procedur, itp.*). Niezależnie od przyjętej metodyki ocen, ma ona wskazać te obszary, które wymagają szczególnej uwagi ze strony Administratora Danych Osobowych (dalej: ADO) lub Inspektora Ochrony Danych (dalej: IOD), a także te obszary, do których należy wrócić w przypadku konieczności powtórnego badania, np. po stwierdzeniu istotnych słabości, uchybień lub nieprawidłowości).
   Opcję *NIE DOTYCZY* warto wykorzystywać, gdy badana jednostka nie jest objęta danym wymogiem (np. ze względu na nikłą skalę przetwarzania danych tego typu) albo gdy z innych względów świadomie ograniczono zakres badania.
   Dodatkową pomocą metodyczną jest wskazanie bardziej szczegółowych (111) wymogów, które wynikają z RODO, uodo albo zidentyfikowanej dobrej praktyki (ocena: *TAK*, *NIE*, *ND.*, *W REALIZACJI*). **Ocena spełniania poszczególnych wymogów ma wspomagać audytora lub kontrolera w dokonaniu oceny danego obszaru**.
   Należy jednak pamiętać, że w każdym przypadku ocena obszaru powinna uwzględniać kontekst danego ustalenia, a w szczególności charakter DO, zakres ich przetwarzania oraz przyczyny i skutki ewentualnych niezgodności z wymogami. Dlatego też, nie we wszystkich przypadkach brak spełniania wymogów będzie się kończyć oceną negatywną albo zastrzeżeniami. Dotyczy to zwłaszcza przypadków, gdy nie zmniejszyła się ochrona praw i wolności osób których przetwarzanie dotyczy.

6. Podsumowaniem formularza jest ocena ogólna, znajdująca się na jego końcu. **Ocena ogólna powinna podsumować funkcjonowanie systemu ochrony DO oraz odnieść się do najważniejszych kwestii, problemów, uwag i zastrzeżeń**. Można w niej również zaznaczyć czy, kiedy oraz w jakim obszarze ocena systemu powinna zostać powtórzona. Pomocą dla formułowania oceny ogólnej jest tabela podsumowująca liczbę ocen. Uzyskane dane ilościowe mogą być użyteczną pomocą poglądową, jednak każdorazowo należy uwzględnić, że nie odzwierciedlają one w pełni rozłożenia ryzyka związanego z ocenami negatywnymi uzyskanymi w konkretnych dla danej jednostki obszarach. Ryzyko to nie jest równomiernie rozłożone na wszystkie obszary. W zależności od badanej jednostki (tj. rodzaju DO oraz charakterystyki ich przetwarzania) inne obszary mogą być uznane za kluczowe i to oceny w tych obszarach będą decydować o ocenie ogólnej.
   Ocena ogólna ułatwia odniesienie jej do ocen poszczególnych obszarów oraz konkretnych wymogów. Jednak zamieszczenie jej w formularzu nie jest konieczne, zwłaszcza jeżeli ocena albo stosowne podsumowanie badanych obszarów zostanie zamieszczone w innym dokumencie (np. raporcie, sprawozdaniu lub wystąpieniu pokontrolnym). W takich przypadkach niniejszy formularz służy jedynie jako pomoc / narzędzie w audycie albo kontroli i należy go odpowiednio zmodyfikować.

Ocena spełniania obowiązków w zakresie ochrony danych osobowych w *(nazwa organu, jednostki, komórki organizacyjnej)*

A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
I. ORGANIZACJA SYSTEMU OCHRONY DANYCH OSOBOWYCH							
I.1 Polityka w zakresie ochrony DO (procedury przetwarzania DO)	[ocena obszaru]	1. Czy opracowano i wdrożono politykę ochrony danych osobowych?	[ocena wymogu]			Informacja od ADO, IOD i pracownika ds. IT. Weryfikacja polityki w zakresie bezpieczeństwa i ochrony DO. Potwierdzenie istnienia procedur dot. SZBI, inna dokumentacja lub dane potwierdzające, w szczególności dokumentacja: - opisująca procedury przetwarzania danych; - wskazująca działania, jakie należy podjąć (np. nadawanie praw dostępu, monitorowanie incydentów, back up, mechanizmy kryptograficzne, testy bezpieczeństwa, audyty, kontrole itp.); - określająca zasady i reguły postępowania, jakie należy zastosować. Istniejąca dokumentacja analizy ryzyka dla ochrony DO - kwerenda wyników analizy ryzyka z ostatniego okresu z uwzględnieniem rekomendacji odnoszących się do środków technicznych i organizacyjnych, zapewniających ochronę DO. Aktualizacja procedur – ustalenie dat ostatnich przeglądów i aktualizacji procedur. Uwaga: Politykę ochrony danych osobowych stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań z zakresu ochrony danych osobowych w sposób zgodny z prawem i efektywny, w szczególności zapewniający odpowiedni stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych. Politykę ochrony DO może stanowić: - jeden dokument/procedura określająca całościowo ukształtowany w danej jednostce system ochrony DO, lub - suma szeregu dokumentów/procedur normujących w danym obszarze kwestie przetwarzania DO (np. instrukcja kancelaryjna, procedury rozpatrywania skarg i wniosków, procedury udzielania zamówień publicznych lub procedury projektowania systemów teleinformatycznych).	*art. 24 i 32 RODO;* *mot. 26, 28, 29, 39, 74-78, 83 i 85 preambuły;* *Rozporządzenie KRI* *Standardy KZ*
		2. Czy polityka ochrony DO, procedury wewnętrzne albo powtarzalne praktyki uwzględniają najważniejsze kwestie dotyczące zabezpieczeń organizacyjnych, mających wpływ na bezpieczeństwo przetwarzanych DO? W szczególności, czy odnoszą się do: a) wykorzystania pseudonimizacji i szyfrowania DO w systemach i aplikacjach IT? b) konieczności ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania DO? c) zdolności do szybkiego przywrócenia dostępności DO i dostępu do nich w razie incydentu fizycznego lub technicznego? d) regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?	[ocena wymogu]				
		3. Czy polityka ochrony DO podlega przeglądom i jest okresowo aktualizowana?	[ocena wymogu]				
I.2 Wyznaczenie ADO	[ocena obszaru]	Czy w jednostce nastąpiło powierzenie zadań ADO wyznaczonym podmiotom (osobom/stanowiskom/usługodawcom)? Czy zadania te zostały powierzone w formie pisemnej?	[ocena wymogu]			Informacja od ADO lub IOD, dokument potwierdzających wyznaczenie IOD, zakres obowiązków, opis stanowiska pracy, umowa o świadczenie usług zawarta z osobą fizyczną lub innym podmiotem. Wskazanie osób/komórek organizacyjnych/podmiotów, którym powierzono zadania ADO w procedurach ODO.	*art. 4 pkt 7 RODO*
I.3 Szkolenia pracowników	[ocena obszaru]	Czy pracownicy jednostki zostali przygotowani do realizacji obowiązków zgodnie z zasadami RODO? W szczególności, czy zorganizowano szkolenia z zakresu przepisów o ochronie DO dla osób pełniących funkcje ADO, IOD oraz pracowników uczestniczących w przetwarzaniu DO?	[ocena wymogu]			Informacja od ADO i IOD. Plan szkoleń/sprawozdania. Dokumentacja potwierdzająca przeprowadzenie szkoleń, spotkań (w tym ich zakres).	*art. 36a ust. 2 lit. c uodo;* *wytyczne dot. IOD*
I.4 Upoważnienie do przetwarzania DO	[ocena obszaru]	1. Czy DO są przetwarzane wyłącznie przez osoby/podmioty działające na polecenie i z upoważnienia ADO oraz wyłącznie w zakresie niezbędnym do realizacji swoich zadań?	[ocena wymogu]			Informacja od ADO. W celu weryfikacji sposobu dokumentowania wydawania upoważnień do przetwarzania można poprosić o rejestr przetwarzania oraz o zestawienie wszystkich upoważnionych osób. Należy również zwrócić uwagę na status upoważnień wydanych przed wejściem w życie RODO. Jeżeli nie zostały odwołane i są ważne, to czy zostały uwzględnione w aktualnej dokumentacji przetwarzania oraz czy spełniają wymogi RODO (integralność i poufność przetwarzania DO). Uwaga: ADO oraz podmiot przetwarzający podejmują działania w celu zapewnienia by każdy podmiot działający z upoważnienia ADO lub podmiotu przetwarzającego, który ma dostęp do DO, przetwarzał je wyłącznie na polecenie administratora, chyba, że wymaga tego od niego prawo.	*art. 32 ust. 4 RODO*
		2. Czy ADO dokumentuje proces upoważniania do przetwarzania DO w sposób, który umożliwia ustalenie wszystkich osób zaangażowanych w procesy przetwarzania DO?	[ocena wymogu]				

	A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
I.5	Współadministrowanie DO	[ocena obszaru]	1. Czy jednostka zidentyfikowała wszystkie procesy przetwarzania DO, które mają więcej niż jednego ADO?	[ocena wymogu]			Informacja od ADO i IOD, Rejestr czynności przetwarzania, dokumentacja z inwentaryzacji procesów etc. Uwaga: Jeśli odpowiedź na to pytanie brzmi "NIE DOTYCZY" to nie ma konieczności weryfikowania pozostałych pytań w obszarze I.5. Współadministrowanie DO	*art. 26 RODO dobra praktyka*
			2. Czy w przypadku współadministrowania, cele i sposoby przetwarzania zostały określone wspólnie przez wszystkich współadministratorów?	[ocena wymogu]			Informacja od IOD. Dokumentacja z określenia celów i sposobów przetwarzania lub regulacje prawne. Analiza umów/porozumień, przepisy w aktach prawnych lub inne dokumenty potwierdzające.	*art. 26 ust. 1 RODO; mot. 79 preambuły.*
			3. Czy zakresy odpowiedzialności dotyczącej wypełniania obowiązków przez współadministratorów: - zostały określone w sposób przejrzysty oraz - należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą?	[ocena wymogu]			Informacja od ADO i IOD. Weryfikacja uzgodnień między administratorami. Analiza dokumentacji określającej zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi, np. umowy/ porozumienia zawierające kwestie związane ze współadministrowaniem. Uwaga: W szczególności należy zwrócić uwagę na zakresy odpowiedzialności współadministratorów w odniesieniu do: - wykonywania praw osoby, której dane dotyczą, w tym do - obowiązków informacyjnych, o których mowa w art. 13 i 14.	*art. 26 RODO; mot. 79 preambuły.*
			4. Czy wskazano punkt kontaktowy dla osób, których dane dotyczą? Czy zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą?	[ocena wymogu]			Informacja od współadministratorów i IOD. Analiza treści dokumentacji związanej ze współadministrowaniem. Weryfikacja wskazania/dostępności punktu kontaktowego.	*art. 26 RODO*
I.6	Podmioty przetwarzające	[ocena obszaru]	Czy w jednostce zidentyfikowano wszystkie procesy przetwarzania DO, w których przetwarzanie jest dokonywane przez podmiot przetwarzający? Czy zidentyfikowano wszystkie podmioty przetwarzające oraz wszystkie inne podmioty (usługodawców) przetwarzające w ich imieniu?	[ocena wymogu]			Informacja od ADO i IOD. Weryfikacja rejestrów DO oraz analiza umów zawartych z podmiotami przetwarzającymi. Wykaz wszystkich podmiotów przetwarzających procesy przetwarzania danych ADO. Przykłady powierzenia przetwarzania to np.: a. powierzenie archiwizacji, b. usługi serwisowe systemów IT, c. serwisowanie systemu obsługi kasy zapomogowo-pożyczkowej, d. umowy na testy penetracyjne, e. zlecenie wyrobienia pieczątek.	*art. 28 RODO;* *mot. 81 preambuły;*
I.8	Umocowanie podmiotów przetwarzających	[ocena obszaru]	Czy wszystkie podmioty przetwarzające DO (w tym inne podmioty przetwarzające, które wykonują usługi na ich rzecz) zostały upoważnione przez ADO? Czy przetwarzanie DO zostało powierzone w formie pisemnej, w tym elektronicznej (np. zgoda ADO, umowa albo inny akt prawny)?	[ocena wymogu]			Informacja od ADO i IOD. Weryfikacja rejestrów czynności przetwarzania DO oraz analiza umów zawartych z podmiotami przetwarzającymi. Wykaz wszystkich podmiotów przetwarzających DO. Analiza treści zgód wydanych przez ADO, informacje od podmiotów przetwarzających oraz ewentualne sprzeciwy ADO wobec zmian w zakresie podmiotów przetwarzających.	*art. 28 ust. 2-4, art. 30 RODO;* *mot. 81 preambuły; Standardy KZ*
I.9	Nadzór nad umowami przetwarzania DO	[ocena obszaru]	1. Czy dokonano inwentaryzacji umów powierzenia DO?	[ocena wymogu]				
			2. Czy wypracowano w jednostce wzory umów albo klauzul umownych związanych ze świadczeniem usług przetwarzania DO? Czy są one prawidłowe?	[ocena wymogu]				

A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
I.10 Umowy o przetwarzanie DO	[ocena obszaru]	1. Czy umowy dot. przetwarzania DO dookreślają zgodę albo brak zgody na korzystanie z innych podmiotów przetwarzających? (art. 28 ust. 2 i 4 RODO)	[ocena wymogu]			Informacja od ADO i IOD. Weryfikacja rejestrów DO oraz analiza wybranych umów zawartych z podmiotami przetwarzającymi na podstawie doboru próby. Wykaz wszystkich podmiotów przetwarzających procesy przetwarzania danych. Uwaga: Elementy wymienione w art. 28 RODO, które powinny się znaleźć w umowie nie tworzą zamkniętego katalogu. W każdym przypadku o tym co powinno się znaleźć w umowie a co nie jest istotne decyduje konkretny charakter przetwarzanych danych (np. dane wrażliwe) oraz sposób ich przetwarzania (np. z wykorzystaniem internetu). Podczas doboru próby umów do badania szczegółowego należy uwzględnić również umowy zawarte przed wejściem w życie RODO. Podjęcie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku naruszenia praw i wolności osób, których dane dotyczą – dot. umów outsourcingu utrzymania infrastruktury IT. Jeśli odpowiedź na to pytanie brzmi "NIE DOTYCZY to nie ma konieczności weryfikowania pozostałych pytań w obszarze I.10. Umowy o przetwarzanie DO.	*art. 28 ust 2-4 i 9, art. 30 ust. 2 oraz art. 32-36 RODO;* *mot. 81 preambuły;*
		2. Czy umowy dot. przetwarzania DO (art. 28 ust. 3 RODO) określają: - przedmiot i czas trwania przetwarzania, - charakter i cel przetwarzania, - rodzaj DO oraz kategorie osób, których dotyczą, - obowiązki i prawa ADO, - osoby odpowiedzialne i właściwe do kontaktów roboczych po stronie ADO i podmiotu przetwarzającego?	[ocena wymogu]				
		3. Czy przetwarzanie przez podmiot przetwarzający (w tym w zakresie przekazywania ich państwu trzeciemu) zostało ograniczone do jedynie udokumentowanych poleceń administratora? (art. 28 ust. 3 RODO lit. a)	[ocena wymogu]				
		4. Czy zobowiązano podmiot przetwarzający do zachowania tajemnicy albo poinformowano go o istnieniu takiego obowiązku? (art. 28 ust. 3 RODO lit. b)	[ocena wymogu]				
		5. Czy zobowiązano podmiot przetwarzający do podjęcia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób, których dane dotyczą, a w szczególności zapewnienie: (art. 28 ust. 3 RODO lit. c) - pseudonimizacji i szyfrowania DO, - poufności, integralności, dostępności i odporności systemów i usług przetwarzania, - zdolności szybkiego przywrócenia dostępności DO w razie incydentu fizycznego lub technicznego, - regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?	[ocena wymogu]				
		6. Czy zobowiązano podmiot przetwarzający do przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego? (art. 28 ust. 3 RODO lit. d)	[ocena wymogu]				
		7. Czy zobowiązano podmiot przetwarzający do wspomagania ADO, w tym do zapewnienia odpowiednich środków technicznych i organizacyjnych do wywiązywania się z obowiązku odpowiadania na żądania oraz do wykonywania praw osób, których danych dotyczą? (art. 28 ust. 3 RODO lit. e)	[ocena wymogu]				
		8. Czy zobowiązano podmiot przetwarzający (art. 28 ust. 3 RODO lit. f) do wspomagania ADO w wywiązywaniu się z obowiązków w zakresie zapewnienia bezpieczeństwa DO (art. 32-34 RODO) oraz oceny skutków dla ochrony danych (art. 35-36 RODO), w tym zwłaszcza z: - obowiązku prowadzenia rejestru wszystkich kategorii czynności przetwarzania DO dokonywanych w imieniu ADO (art. 30 ust. 2 RODO), - obowiązku zgłaszania naruszenia ochrony DO (art. 33 ust. 2 RODO), - obowiązku współpracy i udzielania wyjaśnień ADO?	[ocena wymogu]				
		9. Czy zobowiązano podmiot przetwarzający do usunięcia albo zwrotu wszelkich DO oraz ich istniejących kopii po zakończeniu świadczenia usług, z wyjątkiem sytuacji, gdy obowiązek ich przechowywania wynika z przepisów szczególnych? (art. 28 ust. 3 RODO lit. g)	[ocena wymogu]				
		10. Czy zobowiązano podmiot przetwarzający do udostępnienia ADO wszelkich informacji niezbędnych do wykazania obowiązków wynikających z RODO oraz do współpracy, w tym poddania się ewentualnym kontrolom, audytom oraz inspekcjom prowadzonym przez ADO albo wskazane przez niego podmioty? (art. 28 ust. 3 RODO lit. h)	[ocena wymogu]				

	A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
I.11	Przekazywanie do państwa trzeciego lub organizacji międzynarodowej	[ocena obszaru]	1. W przypadku przekazywania danych do państw trzecich lub organizacji międzynarodowych: Czy ustalono osoby odpowiedzialne za podejmowanie decyzji w tym zakresie oraz wewnętrzne procedury postępowania?	[ocena wymogu]			Informacja od ADO i IOD. Weryfikacja procedur. Przegląd procesów dotyczących przetwarzania danych, które są albo będą przekazywane do państw trzecich lub organizacji międzynarodowych. Uwaga: Przekazanie DO, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej następuje tylko, gdy (z zastrzeżeniem innych przepisów RODO) ADO i podmiot przetwarzający spełnią warunki określone w art. 44-50 RODO, w tym warunki dalszego przekazania danych z państwa trzeciego lub przez organizację międzynarodową do innego państwa trzeciego lub innej organizacji międzynarodowej. Jeśli odpowiedź na to pytanie brzmi "NIE DOTYCZY to nie ma konieczności weryfikowania pozostałych pytań w obszarze I.11. Przekazywanie do państwa trzeciego lub organizacji międzynarodowej.	*art. 44-49 RODO;* *mot. 6, 101-116 preambuły.*
			2. W przypadku przekazywania danych do państw trzecich lub organizacji międzynarodowych: Czy przekazywanie następuje po wykazaniu przez ADO albo podmiot przetwarzający, że: a) według Komisji Europejskiej, państwo trzecie lub dana organizacja międzynarodowa zapewnia odpowiedni stopień ochrony, b) zapewniono odpowiednie zabezpieczenia (w tym reguły korporacyjne), prawa osób, których dane dotyczą oraz skuteczne środki ochrony prawnej, c) państwo członkowskie lub organ nadzorczy wydało zezwolenie na podstawie art. 26 ust. 2 dyrektywy 95/46/WE do czasu zmiany, zastąpienia lub uchylenia zezwolenia (art. 46 ust. 5 RODO), lub d) spełniono jeden z warunków wymienionych w art. 49 RODO (tj. wyjątek w szczególnych sytuacjach).	[ocena wymogu]			Informacja od ADO i IOD. Uwaga: Zgodnie z art. 45 ust. 8 RODO Komisja publikuje w Dzienniku Urzędowym Unii Europejskiej i na swojej stronie internetowej wykaz państw trzecich, terytoriów i określonych sektorów w państwie trzecim oraz organizacji międzynarodowych, co do których przyjęła decyzję stwierdzającą odpowiedni stopień ochrony lub jego brak. Art. 46 ust. 2 RODO wymienia odpowiednie zabezpieczenia, które gwarantują ochronę DO w przypadku ich przekazywania. W przypadku pozostałych zabezpieczeń konieczne jest zezwolenie PUODO (art. 46 ust. 3).	
	II. PRAWO DO PRZETWARZANIA DANYCH OSOBOWYCH							
II.1	Podstawa prawna przetwarzania DO	[ocena obszaru]	Czy dla wszystkich zbiorów danych/procesów przetwarzania danych zidentyfikowano podstawę prawną (warunki przetwarzania)? Czy zostało to udokumentowane w rejestrze czynności przetwarzania DO?	[ocena wymogu]			Wywiady z IOD i pozostałymi kierownikami właściwych komórek organizacyjnych. Przegląd rejestru czynności przetwarzania DO oraz przegląd zawartych tam podstaw prawnych upoważniających do przetwarzania DO (podanie przepisu prawa, umowy lub zgody). Porównanie rejestru z wybranymi czynnościami przetwarzania DO.	*Warunki przetwarzania (art. 6 RODO), szczegółowe i dodatkowe warunki przetwarzania DO (art. 8-10 RODO mot. 40-57 preambuły).*
II.2	Identyfikacja celów przetwarzania DO	[ocena obszaru]	1. Czy zidentyfikowano określone w prawie cele przetwarzania DO?	[ocena wymogu]			Informacja od ADO i IOD Dokument potwierdzający identyfikację (zestawienia, rejestr czynności przetwarzania DO itp.). Przykłady procesów: ZFŚS, rekrutacja, umowy cywilnoprawne pod warunkiem, że chcemy przetwarzać dane w innym celu niż tylko zawarcie umowy.	*art. 6 ust. 3 RODO*
			2. Jeżeli cel przetwarzania DO nie został określony w prawie, to czy przetwarzanie to jest niezbędne dla realizacji interesu publicznego lub władzy publicznej?	[ocena wymogu]				
II.3	Zgoda na przetwarzanie DO	[ocena obszaru]	1. Czy zidentyfikowano DO, dla których podstawą przetwarzania jest zgoda?	[ocena wymogu]			Informacja od ADO lub IOD. Dobrą praktyką jest określenie wzoru zgody uwzględniającego wymogi RODO. Badanie powinno w szczególności objąć sprawdzenie udzielonych zgód oraz ewentualnego wzoru zgody. Dobrą praktyką jest również sformalizowany system zarządzania zgodami na przetwarzanie danych osobowych, który umożliwia rejestrację zgody, odnalezienie informacji o zgodach udzielonych przez jedną osobę oraz ich wycofanie.	*art. 4 pkt 11 oraz art. 7 RODO;* *mot. 32, 42 i 43 preambuły;*
			2. Jeżeli wyłączną podstawą przetwarzania DO jest zgoda to: a) Czy treść zgody (w szczególności ewentualnego wzoru takiej zgody) pozwala na okazanie woli przetwarzania DO w sposób: - jednoznaczny (tj. konkretnie i wyraźnie odróżniający od pozostałych kwestii), dobrowolny (tj. bez uzależniania zgody od świadczenia usług niepowiązanych z przetwarzaniem danych), - zrozumiały (tj. w łatwo dostępnej formie, sformułowanie jasnym i prostym językiem, bez nieuczciwych warunków), - świadomy (tj. upewnieniem się co do tożsamości ADO oraz zamierzonych celów przetwarzania DO)? b) Czy na wszystkie cele przetwarzania DO uzyskano zgodę osoby, której dane dotyczą? c) Czy poinformowano o prawie do wycofania zgody w dowolnym momencie? d) Czy wykazano (udokumentowano) wyrażenie zgody? e) Czy przewidziano tryb postępowania z DO dotyczącymi dzieci?	[ocena wymogu]				
			3. Czy istnieje system rejestrowania i zarządzania bieżącą zgodą na przetwarzanie DO?	[ocena wymogu]				

	A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
II.4	Spełnienie warunków przetwarzania DO	[ocena obszaru]	Czy dla wybranych procesów przetwarzania DO: a) spełnione zostały warunki przetwarzania, określone w podstawie prawnej przetwarzania, zawartej w rejestrze czynności? b) cele przetwarzania są zgodne z celami, w jakich zostały zebrane? c) dane są przetwarzane w sposób adekwatny, tj. wyłącznie w zakresie niezbędnym do realizacji celów ich przetwarzania? d) dane są przetwarzane w formie umożliwiającej identyfikację osoby, której dane dotyczą?	[ocena wymogu]			Ocena na podstawie wybranych procesów przetwarzania DO.	*art. 5, 6 i 11 RODO;* *mot. 39-48 oraz 50 preambuły.*
II.5	Zaprzestanie przetwarzania DO	[ocena obszaru]	Czy zaprzestano przetwarzania DO niezwłocznie po stwierdzeniu: - braku podstaw do ich przetwarzania? - niezgodności celów przetwarzania DO z celami, w którym zostały zebrane?	[ocena wymogu]			Badanie wybranych przypadków po stwierdzeniu, że brak jest podstaw do dalszego przetwarzania DO.	*art. 6 RODO*
III.	**III. REALIZACJA PRAW OSOBY, KTÓREJ DANE DOTYCZĄ**							
III.1	Procedura udzielania informacji osobom, których dane dotyczą DO	[ocena obszaru]	Czy opracowano procedurę udzielania informacji osobom, których dotyczą DO?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd ustanowionych procedur.	*art. 5 ust. 1, 12, 13, 14, 15 RODO;* *mot. 39, 58, 59, 60, 61, 64, 68 preambuły;* *art. 3 ust. 3, art.. 4 ust 3 uodo*
III.2	Obowiązki informacyjne podczas pozyskiwania DO od osób, których dane dotyczą (klauzula informacyjna)	[ocena obszaru]	1. Czy opracowano treść klauzuli informacyjnej dla osób, od których DO będą pozyskiwane oraz czy jej treść spełnia wymogi RODO?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd i analiza klauzul.	*art. 13 RODO; mot. 39, 58-63 preambuły*
			2. Czy przewidziano obowiązek przedstawienia stosownych informacji (klauzuli informacyjnej) najpóźniej w czasie pozyskiwania DO? Czy przewidziano możliwość odstąpienia od tego obowiązku po upewnieniu się, że osoba, której dane dot. dysponuje już tymi informacjami?	[ocena wymogu]				
			3. Czy wzór klauzuli zapewnia przedstawienie: a) tożsamości i danych kontaktowych ADO; b) danych kontaktowych IOD, gdy ma to zastosowanie; c) celów przetwarzania oraz podstawy prawnej przetwarzania; d) wykazania prawnie uzasadnionych interesów (jeżeli są one podstawą przetwarzania); e) odbiorców danych; f) ewentualnym zamiarze przekazywania danych do państwa trzeciego lub organizacji międzynarodowej oraz podjętych zabezpieczeniach w tym zakresie (patrz szczegółowo art. 14 ust. 1 lit. f RODO)?	[ocena wymogu]				
			4.Czy wzór klauzuli zapewnia rzetelność i przejrzystość przetwarzania DO poprzez przedstawienie informacji o: a) okresie przechowywania danych lub (jeżeli nie jest to możliwe) kryteria ustalania tego okresu; b) prawach dostępu do danych, sprostowania, usunięcia, ograniczenia, przetwarzania, wniesienia sprzeciwu i przenoszenia danych; c) prawie cofnięcia zgody na przetwarzanie danych (jeżeli jest ona jedyną podstawą dla ich przetwarzania); d) prawie wniesienia skargi do organu nadzorczego; e) przyczynach zażądania podania DO (np. wymóg ustawowy, umowny albo konieczność realizacji umowy/usługi), czy jest to obowiązkowe oraz o ewentualnych skutkach niepodania DO; f) ewentualnym zautomatyzowanym podejmowaniu decyzji na podstawie DO, w tym o profilowaniu oraz o zasadach podejmowania tych decyzji, a także o znaczeniu i ewentualnych konsekwencjach dla osoby, której dane dotyczą.	[ocena wymogu]				

A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
III.3 Obowiązki informacyjne podczas pozyskiwania DO w inny sposób niż bezpośrednio od osób, których dane dotyczą (klauzula informacyjna)	**[ocena obszaru]**	1. Czy opracowano klauzulę informacyjną dla osób, których dane będą przetwarzane, a których dane pozyskano w sposób inny niż od osoby, której dane dotyczą?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd wdrożonych klauzul.	*art. 12, 14 ust. 3 pkt a-c i ust.5, i art. 15 ust. 3 RODO;* *mot. 39, 58, 59,60,64,68 preambuły;* *art. 4 uodo;*
		2. Czy przewidziano obowiązek przedstawienia stosownej informacji (klauzuli informacyjnej) w rozsądnym terminie oraz najpóźniej: - w ciągu miesiąca od ich pozyskania, - przy pierwszej komunikacji lub - przy pierwszym ujawnieniu DO innemu odbiorcy?	[ocena wymogu]				
		3. Czy przewidziano możliwość odstąpienia od ww. obowiązku po upewnieniu się, że (art. 14 ust. 5 RODO): - osoba, której dane dot. dysponuje już tymi informacjami? - udzielenie informacji jest niemożliwe albo wymaga niewspółmiernie dużego wysiłku? - pozyskanie lub ujawnienie jest wyraźnie uregulowane prawem? - zgodnie z prawem DO muszą pozostać poufne?	[ocena wymogu]				
		4. Czy przewidziano możliwość odstąpienia od ww. obowiązku po upewnieniu się, że (art. 4 uodo) służy to realizacji zadania publicznego, jest to niezbędne dla realizacji celów, publicznych wymienionych w art. 23 ust. 1 RODO tylko w przypadkach, gdy przekazanie tych informacji uniemożliwi lub znacząco utrudni wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji realizowanego zadania publicznego lub naruszy ochronę informacji niejawnych?	[ocena wymogu]				
		5. Czy wzór klauzuli zapewnia informację o: a) tożsamości i danych kontaktowych ADO lub jego przedstawiciela, b) danych kontaktowych IOD (jeżeli został powołany), c) celach i podstawach prawnych przetwarzania DO, d) kategoriach odnośnych DO, e) informacjach o odbiorcach lub kategoriach odbiorców DO, f) ewentualnym zamiarze przekazywania danych do państwa trzeciego lub organizacji międzynarodowej oraz podjętych zabezpieczeniach w tym zakresie (patrz szczegółowo art. 14 ust. 1 lit. f RODO)?	[ocena wymogu]				
		6. Czy wzór klauzuli zapewnia rzetelność i przejrzystość przetwarzania DO poprzez przedstawienie dodatkowych informacji o: a) okresie przechowywania DO lub kryteriach ustalania tego okresu, b) prawnie uzasadnionym interesie ADO lub osoby trzeciej (jeżeli są one podstawą przetwarzania), c) prawie dostępu do danych, sprostowania, usunięcia, ograniczenia przetwarzania oraz wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, d) prawie do cofnięcia zgody w dowolnym momencie (jeżeli jest ona podstawą dla ich przetwarzania), e) prawie wniesienia skargi do organu nadzorczego, f) źródle pochodzenia DO oraz o pochodzeniu ich ze źródeł publicznie dostępnych (jeżeli miało to zastosowanie), g) ewentualnym zautomatyzowanym podejmowaniu decyzji na podstawie DO, w tym o profilowaniu oraz o zasadach podejmowania tych decyzji, a także o znaczeniu i ewentualnych konsekwencjach dla osoby, której dane dotyczą?	[ocena wymogu]				

A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
III.4 Obowiązki informacyjne wobec osób, których dane były przetwarzane przed wejściem w życie RODO	[ocena obszaru]	1. Czy dokonano przeglądu DO aktualnie przetwarzanych pod względem konieczności wypełnienia obowiązków informacyjnych wobec osób, których dane są przetwarzane?	[ocena wymogu]			Informacja od ADO, IOD, przegląd projektów procedur oraz ewentualnej klauzuli informacyjnej. Dla oceny stopnia wypełnienia obowiązku informacyjnego zastosowanie znajduje treść ww. klauzul informacyjnych odnoszących się do pozyskiwania DO w inny sposób, niż bezpośrednio od osób, których dane dotyczą. Uwaga: w zakresie nieuregulowanym w art. 14 ust. 5 RODO ADO wykonujący zadanie publiczne nie przekazuje informacji, jeżeli: **a)** służy to realizacji zadania publicznego **i** **b)** niewykonanie obowiązku jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 RODO [katalog celów publicznych], **oraz** **c)** przekazanie tych informacji: - uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego **lub** - naruszy ochronę informacji niejawnych. ADO jest obowiązany poinformować osobę, której dane dotyczą na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie nieprzekazania informacji, o których mowa w art. 14 ust. 1, 2 i 4 RODO.	*art. 14 RODO*
		2. Czy w przypadku stwierdzenia konieczności dopełnienia obowiązków informacyjnych wobec osób, których dane są już przetwarzane, dopełniono obowiązku informacyjnego, o którym mowa w art. 14 RODO?	[ocena wymogu]				
III.5 Obowiązki informacyjne w przypadku zmiany celu przetwarzania DO.	[ocena obszaru]	1. Czy procedura udzielania informacji przewiduje obowiązek ponownego zastosowania klauzuli informacyjnej wobec osób, których DO zostały zebrane w innym celu niż zamierzony cel ich wykorzystania?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd projektów klauzul.	*art. 13 ust. 3 RODO;* *art. 3 uodo*
		2. Czy procedura ta uwzględnia odstąpienie od ww. obowiązku gdy zmiana celu przetwarzania służy realizacji zadania publicznego i niewykonanie obowiązku jest niezbędne dla realizacji celów publicznych, o których mowa w art. 23 ust. 1 RODO oraz przekazanie tych informacji: (a) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub (b) naruszy ochronę informacji niejawnych.	[ocena wymogu]				
III.6 Prawo dostępu do DO	[ocena obszaru]	1. Czy zapewniono realizację praw dostępu dla osób, których DO dotyczą, w tym czy wskazano podmiot właściwy w zakresie potwierdzania przetwarzania DO oraz udzielający dostępu do informacji o: a) celach przetwarzania DO, b) kategoriach odnośnych DO, c) odbiorcach lub kategoriach odbiorców, którym DO zostały lub zostaną ujawnione, d) planowanym okresie przechowywania DO, a gdy nie jest to możliwe, kryteriach ustalania tego okresu, e) prawie do żądania od ADO sprostowania, usunięcia lub ograniczenia przetwarzania DO oraz do wniesienia sprzeciwu wobec takiego przetwarzania, f) prawie wniesienia skargi do organu nadzorczego, g) ewentualnych informacjach nt. źródła pozyskania DO, h) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz o zasadach podejmowania tych decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania, i) odpowiednich zabezpieczeniach, w przypadku gdy DO są przekazywane do państwa trzeciego lub organizacji międzynarodowej.	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur. Uwaga: Niektóre z praw mogą być ograniczone przez szczegółowe prawodawstwo odnoszące się do konkretnych branż - polskie albo UE (patrz art. 23 RODO). W przypadku, gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1 i 3 RODO, wymaga niewspółmiernie dużego wysiłku związanego z wyszukaniem danych osobowych, ADO wykonujący zadanie publiczne wzywa osobę, której dane dotyczą, do udzielenia informacji pozwalających na wyszukanie tych danych. Stosuje się odpowiednio przepis art. 64 Kodeks postępowania administracyjnego (art. 5 ust. 2 *uodo*). ADO jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie niewykonania obowiązków, o których mowa w art. 15 ust. 1-3 RODO (art. 5 ust. 4 *uodo*).	*art. 15 RODO;* *art. 5 uodo;* *mot. 59, 63, 64 i 73 preambuły;* *wytyczne dot. przenoszenia.*
		2. Czy przewidziano procedurę dla dostarczania kopii DO podlegających przetwarzaniu, w tym czy wskazano osoby za to odpowiedzialne?	[ocena wymogu]				
		3. Czy procedury uwzględniają możliwość wykorzystania drogi elektronicznej oraz konieczność udzielenia odpowiedzi bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?	[ocena wymogu]				
		4. Czy procedury przewidują możliwość odstąpienia od potwierdzania przetwarzania DO, gdy służy to realizacji zadania publicznego i niewykonanie tego potwierdzenia jest niezbędne dla realizacji celów publicznych, o których mowa w art. 23 ust. 1 RODO, oraz wykonanie tych obowiązków: - uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub - naruszy ochronę informacji niejawnych.	[ocena wymogu]				

A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
III.7 Prawo do sprostowania i usuwania danych	[ocena obszaru]	1. Czy przewidziano procedury ułatwiające realizację wniosku o sprostowanie albo usunięcie DO podlegających przetwarzaniu?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur. Uwaga: Niektóre z praw mogą być ograniczone przez szczegółowe prawodawstwo odnoszące się do konkretnych branż - polskie albo UE (patrz art. 23 RODO). W przypadku, gdy wykonanie obowiązków, o których mowa w art	*art. 16, 17 , 19 i 23 RODO;* *mot. 39, 59, 65, 66 156 preambuły.*
		2. Czy wskazano osoby odpowiedzialne za dokonanie oceny konieczności i możliwości dokonania sprostowania albo usunięcia danych?	[ocena wymogu]				
		3. Czy przewidziano obowiązek powiadomienia każdego odbiorcy, któremu ujawniono DO o fakcie ich sprostowania lub usunięcia?	[ocena wymogu]				
		4. Czy procedury te uwzględniają możliwość wykorzystania drogi elektronicznej oraz odpowiedź bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?	[ocena wymogu]				
III.8 Prawo do ograniczenia przetwarzania	[ocena obszaru]	1. Czy przewidziano procedury ułatwiające realizację wniosku o ograniczenie przetwarzania DO?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur. Uwaga: Niektóre z praw mogą być ograniczone przez szczegółowe prawodawstwo odnoszące się do konkretnych branż - polskie albo UE (patrz art. 23 RODO).	*art. 18, 19 i 23 RODO;* *mot. 59, 67, 156 preambuły.*
		2. Czy wskazano osoby odpowiedzialne za dokonanie oceny konieczności i możliwości ograniczenia przetwarzania DO oraz za ograniczenie przetwarzania tych danych?	[ocena wymogu]				
		3. Czy przewidziano obowiązek powiadomienia każdego odbiorcy, któremu ujawniono DO o fakcie ich sprostowania lub usunięcia?	[ocena wymogu]				
		4. Czy procedury uwzględniają możliwość wykorzystania drogi elektronicznej oraz odpowiedź bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?	[ocena wymogu]				
III.9 Prawo do przenoszenia danych	[ocena obszaru]	1. Czy przewidziano procedury ułatwiające realizację wniosku o przeniesienie DO?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur. Uwaga: prawo dot. wyłącznie danych przetwarzanych w sposób zautomatyzowany na podstawie zgody albo umowy. Ponadto prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Ado. Ponadto niektóre z praw mogą być ograniczone przez szczegółowe prawodawstwo odnoszące się do konkretnych branż - polskie albo UE (patrz art. 23 RODO).	*art. 20 i 23 RODO;* *mot. 59, 68, 156 preambuły;* *wytyczne dot. przenoszenia.*
		2. Czy wskazano osoby odpowiedzialne za dokonanie oceny konieczności i możliwości przeniesienia DO oraz przeniesienie tych danych?	[ocena wymogu]				
		3. Czy procedury uwzględniają możliwość wykorzystania drogi elektronicznej oraz odpowiedź bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?	[ocena wymogu]				
III.10 Prawo sprzeciwu wobec przetwarzania danych w zakresie profilowania oraz marketingu bezpośredniego	[ocena obszaru]	1. Czy przewidziano procedury ułatwiające rozpatrzenie sprzeciwu wobec przetwarzania DO: - w tym profilowania w ramach realizacji interesu publicznego, sprawowania władzy publicznej lub prawnie uzasadnionych interesów ADO; - na potrzeby marketingu bezpośredniego, w tym profilowania?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur. Uwaga: Niektóre z praw mogą być ograniczone przez szczegółowe prawodawstwo odnoszące się do konkretnych branż - polskie albo UE (patrz art. 23 RODO).	*art. 21 i 23 RODO;* *mot. 59, 65, 70 i 73 preambuły.*
		2. Czy wskazano osoby odpowiedzialne za dokonanie oceny konieczności zaprzestania przetwarzania DO, w tym profilowania?	[ocena wymogu]				
		3. Czy procedury uwzględniają możliwość wykorzystania drogi elektronicznej oraz odpowiedź bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?	[ocena wymogu]				

	A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
III.11	Prawo do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowany przetwarzaniu, w tym profilowaniu	[ocena obszaru]	1. Jeżeli w jednostce stosuje się zautomatyzowane podejmowanie decyzji na podstawie DO, to czy zapewniono procedury umożliwiające wyłączenie zainteresowanej osoby z automatycznego przetwarzania, w tym profilowania?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur. Uwaga: Niektóre z praw mogą być ograniczone przez szczegółowe prawodawstwo odnoszące się do konkretnych branż - polskie albo UE (patrz art. 23 RODO).	*art. 22 i 23 RODO;* *mot. 71, 72 preambuły*
			2. Czy wskazano osoby odpowiedzialne za dokonanie oceny konieczności zaprzestania przetwarzania DO, w tym profilowania?	[ocena wymogu]				
			3. Czy procedury uwzględniają możliwość wykorzystania drogi elektronicznej oraz odpowiedź bez zbędnej zwłoki, a najpóźniej w ciągu miesiąca?	[ocena wymogu]				
III.12	Przygotowanie DO do realizacji praw osób, których te dane dotyczą	[ocena obszaru]	Czy dokonano przeglądu procesów przetwarzania DO, w tym przetwarzających je systemów informatycznych w zakresie sprawnego zlokalizowania DO w celu realizacji praw osób, których dane dotyczą, w tym prawa: - dostępu do DO, - sprostowania i usuwania danych, - ograniczenia przetwarzania, - przeniesienia danych, - sprzeciwu wobec przetwarzania danych w zakresie profilowania oraz marketingu bezpośredniego, - wyłączenia od zautomatyzowanego przetwarzania danych?	[ocena wymogu]			Informacja od ADO, IOD i pracownika ds. IT, przegląd procedur, przegląd systemów IT oraz wybranych procesów przetwarzania DO.	*art. 20 ust. 2, 21 ust. 5 RODO*
IV. INSPEKTOR OCHRONY DANYCH								
IV.1	Powołanie IOD	[ocena obszaru]	1. Czy kierownik jednostki wyznaczył IOD?	[ocena wymogu]			Informacja od ADO lub IOD, dokument potwierdzających wyznaczenie IOD, zakres obowiązków, opis stanowiska pracy, umowa o świadczenie usług zawartej z osobą fizyczną lub innym podmiotem. Uwaga, wyznaczenie IOD jest obowiązkowe, gdy: a) przetwarzania dokonują organ lub podmiot publiczny (niezależnie od tego, jakie dane są przetwarzane). Przez podmiot publiczny rozumie się (1) jednostki sektora finansów publicznych, (2) instytuty badawcze, (3) Narodowy Bank Polski. b) główna działalność ADO lub podmiotu przetwarzającego polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; c) główna działalność ADO lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii DO lub DO dotyczących wyroków skazujących i czynów zabronionych. art. 37 ust. 1 RODO. Ponadto zgodnie z art. 10 a) Termin na zawiadomienie PUODO o wyznaczeniu IOD wynosi 14 dni od dnia wyznaczenia i można tego dokonać przez pełnomocnika. b) Wymaga się wskazania: - imienia, nazwiska oraz adresu poczty elektronicznej lub numer telefonu inspektora. - imienia i nazwiska, nazwy albo firmy ADO oraz adresu zamieszkania, siedziby albo miejsca prowadzenia działalności - numeru REGON, jeżeli został nadany ADO lub podmiotowi przetwarzającemu. Zawiadomienia, o których mowa w ust. 1 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. Wg. art. 158 uodo: a) administrator bezpieczeństwa informacji (ABI) zgłoszony do Generalnemu Inspektorowi Ochrony Danych Osobowych (tj. GIODO), do dnia 24 maja 2018 r. staje się IOD; b) aby dotychczasowy ABI stał się IOD na czas nieokreślony należy o tym zawiadomić PUODO do dnia 1 września 2018 r.; c) ADO, który do dnia wejścia w życie nowej uodo nie powołał ABI będzie miał obowiązek wyznaczenia IOD oraz zawiadamia PUODO do dnia 31 lipca 2018 r. Jeśli jednostka nie ma obowiązku powołanie IOD i w związku z tym odpowiedzi na pytania pomocnicze brzmią "NIE DOTYCZY", to nie ma konieczności weryfikowania pozostałych pytań w obszarze V. Inspektor Ochrony Danych.	*art. 37 ust. 1 RODO;* *art. 37 ust. 6 RODO* *mot. 97 preambuły;* *art. 8, 9, 10 i 158 uodo;* *wytyczne dot. IOD*
			2. Czy IOD został powołany w trybie określonym w uodo? W szczególności, czy dopełniono obowiązku zawiadomienia PUODO o powołaniu IOD albo o zmianie danych dot. IOD lub ADO?	[ocena wymogu]				
			3. W przypadku wyznaczenia IOD spoza jednostki, czy powołano pracowników (albo zespół) do kontaktów roboczych ADO z IOD oraz do wypełniania obowiązków związanych z ochroną DO?	[ocena wymogu]			Informacja od ADO i IOD. Analiza umowy o świadczenie usług zawartej z osobą fizyczną lub innym podmiotem spoza organizacji ADO/podmiotu przetwarzającego. Uwaga: dotyczy tylko jednostek, w których IOD został wyznaczony spoza jednostki. Powołanie takiego zespołu nie jest obowiązkowe. Jeśli odpowiedź na to pytanie brzmi "NIE" to nie jest konieczne weryfikowanie pozostałych kwestii dotyczących zespołu	*art. 38 ust. 2 RODO;* *wytyczne dot. IOD.*
			4. Czy wszystkie zadania IOD, o których mowa w art. 39 RODO (albo zadania ww. zespołu) zostały powierzone w formie pisemnej?	[ocena wymogu]			Informacja od ADO i IOD, regulamin organizacyjny, procedury wewnętrzne, umowa, opis stanowiska pracy. Informacja od pracodawcy. Analiza zakresu zadań IOD.	*art. 39 RODO;* *mot. 97 preambuły;* *wytyczne dot. IOD.*

	A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
IV.2	Kompetencje IOD	[ocena obszaru]	1. Czy osoba wyznaczona na IOD posiada odpowiednie kwalifikacje zawodowe, a w szczególności wiedzę nt. prawa i praktyk w dziedzinie ochrony DO oraz realizowanych zadań?	[ocena wymogu]			Informacja od ADO i IOD. Opis stanowiska pracy, cv, życiorys i doświadczenie IOD, szkolenia, dyplomy, certyfikaty zawodowe.	*art. 37 ust. 5 RODO;* *mot. 97 preambuły* *wytyczne dot. IOD.*
			2. Jeżeli IOD jest pracownikiem jednostki, to czy jej kierownictwo uwzględniło potrzeby w zakresie utrzymania wiedzy fachowej (szkoleń i podnoszenia kompetencji)?	[ocena wymogu]			Informacja od ADO (kadry) i IOD. Budżet i plan szkoleń, indywidualny program rozwoju zawodowego, gdy IOD jest pracownikiem ADO. Uwaga: jeżeli IOD pełnił swoją funkcję dłuższy czas, to należy zwrócić uwagę czy był szkolony i podnosił kwalifikacje z zakresu przetwarzania DO? Dopuścić należy również różne formy samokształcenia.	
IV.3	Zasoby IOD	[ocena obszaru]	Czy zapewniono IOD odpowiednie zasoby do wykonywania swoich zadań? W tym zasoby: - kadrowe (np. zespół inspektora ochrony danych)? - infrastrukturalne (pomieszczenia, sprzęt, wyposażenie)? - informatyczne (konto poczty elektronicznej, konto w systemie elektronicznego obiegu dokumentacji)?	[ocena wymogu]			Informacja od ADO i IOD. Uwaga: Należy zwrócić uwagę na skrajnie niewystarczające zasoby IOD do realizacji zwykłych zadań, np. brak wyposażenia albo usytuowanie miejsca stanowiska pracy IOD utrudniające realizację zadań. Powołanie zespołu IOD nie jest obowiązkowe, jednakże warto się zastanowić czy ilość danych przetwarzanych w danej jednostce umożliwi skutecznie wykonywać obowiązki samodzielnie IOD.	*art. 38 ust. 2 RODO;* *wytyczne dot. IOD*
IV.4	Niezależność IOD	[ocena obszaru]	1. Czy IOD jest bezpośrednio podległy najwyższemu kierownictwu jednostki?	[ocena wymogu]			Informacja od ADO i IOD. Statut, regulamin organizacyjny, zakres obowiązków, opis stanowiska pracy.	*art. 38 ust. 3 RODO;* *wytyczne dot. IOD*
			2. Czy pozostałe zadania i obowiązki IOD w jednostce (jeżeli są wykonywane) nie powodują konfliktu interesów z funkcją IOD w jednostce? Np. czy IOD nie zajmuje stanowiska kierowniczego (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy)?	[ocena wymogu]			Informacja od ADO lub IOD. Ponadto zakres zadań IOD, opis stanowiska pracy / umowa o świadczenie usług zawartej z osobą fizyczną lub innym podmiotem spoza organizacji ADO / podmiotu przetwarzającego, w szczególności analiza ich treści.	*art. 38 ust. 6 RODO;* *mot. 97 preambuły;* *wytyczne dot. IOD*
			3. Czy ADO (albo jego przedstawiciel) zapewnił warunki dla niezależnej pracy IOD, w szczególności czy: - powstrzymano się od wydawania instrukcji w zakresie realizacji zadań przez IOD? - nie odwoływano, ani nie karano IOD w związku z wypełnianiem jego zadań?	[ocena wymogu]			Informacja od IOD oraz ewentualne wyjaśnienia od ADO.	*art. 38 ust. 3 RODO;* *mot. 97 preambuły;* *wytyczne dot. IOD.*
IV.5	Dostępność IOD	[ocena obszaru]	1. Czy dopełniono obowiązku zawiadomienia PUODO o danych kontaktowych IOD?	[ocena wymogu]			Informacja od ADO i IOD. Dokument potwierdzający zawiadomienie.	*art. 37 ust. 7, RODO;* *art. 10 uodo;* *wytyczne dot. IOD.*
			2. Czy dopełniono obowiązku publikacji danych kontaktowych IOD? Czy dane te są łatwe do odnalezienia i umożliwiają osobom, których dane dotyczą oraz organom nadzorczym nawiązanie kontaktu w łatwy sposób?	[ocena wymogu]			Informacja od ADO i IOD. Analiza stron www. jednostki, zakładki RODO/ochrona danych osobowych, która uwzględniałaby w szczególności dane osobowe IOD (adres korespondencyjny, telefon kontaktowy lub dedykowany adres email, dedykowana infolinia, formularz kontaktowy z IOD na stronie internetowej organizacji) oraz jego zadania.	*art. 37 ust. 7 RODO;* *art. 11 uodo;* *wytyczne dot. IOD.*
			3. Czy poinformowano pracowników jednostki o imieniu, nazwisku i danych kontaktowych IOD oraz o możliwości konsultacji w zakresie przetwarzania DO?	[ocena wymogu]			Informacja od ADO i IOD. Analiza intranetu jednostki, komunikatów do pracowników, zakładek RODO/ochrona danych osobowych, która uwzględniałaby w szczególności dane osobowe IOD oraz jego zadania.	*wytyczne dot. IOD*
IV.6	Warunki do realizacji zadań IOD	[ocena obszaru]	1. Czy IOD ma możliwość skutecznego, właściwego i niezwłocznego włączenia się we wszystkie procesy przetwarzania danych w jednostce, a w szczególności procesy związane z: a) określaniem zakresu, celów i sposobów tego przetwarzania, b) oceną skutków dla ochrony DO, c) identyfikacją i monitoringiem procesów przetwarzania, d) oceną prawidłowości przetwarzania, e) współpracą i kontaktami z PUODO, f) bezpośrednią obsługą osób, których dane są przetwarzane, g) projektami, programami i zamówieniami publicznymi odnoszącymi się do kwestii przetwarzania DO, h) projektami regulacji prawnych oraz procedur wewnętrznych (tj. realizacją ochrony DO w fazie projektowania).	[ocena wymogu]			Informacja od ADO i IOD. Analiza treści procedur, wytycznych, wskazówek oraz instrukcji wewnętrznych wskazujących na obowiązek współpracy komórek organizacyjnych z IOD w zakresie przetwarzania DO. Uwaga: włączanie IOD w procesy przetwarzania nie oznacza, że może on przejmować kompetencje ADO (jeżeli tak jest patrz punkt wyżej dot. konfliktu interesów IOD).	*art. 38 i 39 RODO;* *mot. 97 preambuły;* *wytyczne dot. IOD.*
			2. Czy procedury wewnętrzne nakładają na pozostałe komórki organizacyjne obowiązek współpracy z IOD, dzięki czemu może on uzyskać niezbędne wsparcie, w szczególności kadrowe, prawne, księgowe oraz informatyczne?	[ocena wymogu]			Informacja od ADO i IOD. Regulaminy organizacyjny i wewnętrzne Polityka/procedury ODO.	*art. 38 ust. 2 RODO;* *wytyczne dot. IOD.*
IV.5	Ocena regulacji wewnętrznych w zakresie ochrony DO przez IOD	[ocena obszaru]	Czy w ocenie IOD obowiązujące w jednostce procedury, polityki wewnętrzne lub powtarzalne praktyki są odpowiednie dla zapewnienia skutecznej ochrony DO?	[ocena wymogu]			Informacja od IOD. Wyniki wcześniejszych audytów/kontroli/sprawdzeń w przedmiotowym obszarze.	*art. 24 ust. 2, 32 i 39 RODO*

	A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
	V. REJESTROWANIE CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH							
V.1	Identyfikacja DO i zakresu ich przetwarzania w jednostce	[ocena obszaru]	Czy dokonano identyfikacji procesów, w których DO są lub będą przetwarzane? Czy zidentyfikowano zakres, w jakim DO są/będą przetwarzane?	[ocena wymogu]			Informacja od ADO i IOD. Przegląd procedur w zakresie przetwarzania DO, badanie wybranych, dokumentów i systemów przetwarzających, procesów przetwarzania danych oraz rejestrów czynności przetwarzania DO.	*Definicja DO oraz ich przetwarzania (art. 4 pkt 1 i 2 RODO).*
V.2	Rejestr czynności przetwarzania DO	[ocena obszaru]	1. Czy wyznaczono podmiot (pracownika albo kom. org.), któremu powierzono przygotowanie/prowadzenie rejestru czynności przetwarzania DO?	[ocena wymogu]			Informacja od ADO i/lub IOD. Analiza/oględziny rejestru. Uwaga: Prowadzenie rejestru czynności przetwarzania nie jest obowiązkiem powszechnym. Zgodnie z art. 30 ust. 5 RODO do prowadzenia rejestru zobowiązani są ADO i podmioty przetwarzające, którzy zatrudniają 250 lub więcej osób oraz gdy: - dokonują systematycznego przetwarzania mogącego powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, lub - dokonują przetwarzania szczególnych kategorii DO, o których mowa w art. 9 ust. 1 RODO, lub - przetwarzają DO dotyczące wyroków skazujących i czynów zabronionych, o czym mowa w art. 10 RODO. Rejestr musi być prowadzony w formie pisemnej, w tym elektronicznej. Dobra praktyka Brytyjskiego Organu nadzorczego ochrony DO do przygotowania się do opracowania rejestru czynności: 1. Nazwy procesów biznesowych; 2. Informacja o podstawie prawnej przetwarzania danych; 3. Informacja o uprawnieniach osób, których dotyczy przetwarzanie danych; 4. Informacja o zautomatyzowanym przetwarzaniu DO w tym o profilowaniu; 5. Źródło, z którego ADO otrzymał DO; 6. Informacja o uzyskaniu zgody na przetwarzanie DO; 7. Miejsce przechowywania danych; 8. Informacja o zidentyfikowanej konieczności przeprowadzenia oceny skutków przetwarzania ochrony danych; 9. Informacja o naruszeniach ochrony DO; 10. Wskazanie technologii, aplikacji lub systemów informatycznych, w których następuje przetwarzanie DO; 11. Termin rozpoczęcia przetwarzania danych. Należy zwrócić uwagę, czy rejestr ten zawiera tylko dane wymagane art. 30 RODO, czy też jednostka rozszerzyła zakres danych ujmowanych w rejestrze? Jeśli tak, to zapytać o motywy rozszerzenia katalogu danych wpisywanych do rejestr (tzn. chodzi o mot./względy praktyczne). Jeżeli jednostka świadomie zaplanowała rozszerzony zakres danych w rejestrze, to może to świadczyć o wyższym poziomie organizacji ochrony DO. Jeżeli brak jest obowiązku prowadzenia danego rejestru, to proszę zaznaczyć "NIE DOTYCZY".	*art. 30 ust. 1 RODO;* *mot. 82 preambuły;* *Standardy KZ.*
			2. Czy jest prowadzony rejestr czynności przetwarzania DO? Czy rejestr jest prowadzony w formie pisemnej, w tym elektronicznej?	[ocena wymogu]				
			3. Czy rejestr zawiera wszystkie elementy wymagane przez art. 30 ust. 1 RODO?	[ocena wymogu]				
V.3	Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu ADO albo przez podmiot przetwarzający	[ocena obszaru]	1. Czy wyznaczono podmiot (pracownika albo kom. org.), któremu powierzono przygotowanie/ prowadzenie rejestru wszystkich kategorii czynności przetwarzania DO?	[ocena wymogu]			Weryfikacja dokumentów dot. rejestru wszystkich kategorii czynności. Weryfikacja zapisów umów powierzenia danych/wzoru umowy powierzenia danych. W przypadku, gdy jednostka jest również podmiotem przetwarzającym dane, to analiza rejestru wszystkich kategorii czynności. Uwaga: Prowadzenie rejestru nie jest obowiązkiem powszechnym. Jeżeli brak jest obowiązku prowadzenia danego rejestru, to należy zaznaczyć "NIE DOTYCZY".	*art. 30 ust. 2 RODO;* *mot. 82 preambuły.*
			2. Czy opracowano rejestr wszystkich czynności przetwarzania DO? Czy jest on prowadzony w formie pisemnej/elektronicznej? Czy zawiera wszystkie elementy wymagane przez art. 30 ust. 2 RODO?	[ocena wymogu]				

A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
VI. OCENA SKUTKÓW PRZETWARZANIA DANYCH OSOBOWYCH							
VI.1 Zarządzanie ryzykiem dla ochrony DO	[ocena obszaru]	1. Czy istnieje procedura (albo powtarzalna praktyka) analizy ryzyka dla ochrony DO?	[ocena wymogu]			Informacja od ADO, IOD i pracownika ds. IT. Weryfikacja polityki w zakresie bezpieczeństwa i ochrony DO. Potwierdzenie istnienia procedur dot. SZBI, inna dokumentacja lub dane potwierdzające, w szczególności dokumentacja: - opisująca procedury przetwarzania danych; - wskazująca działania, jakie należy podjąć (np. nadawanie praw dostępu, monitorowanie incydentów, back up, mechanizmy kryptograficzne, testy bezpieczeństwa, audyty, kontrole itp.); - określająca zasady i reguły postępowania, jakie należy zastosować. Aktualizacja procedur – ustalenie dat ostatnich przeglądów i aktualizacji procedur Istniejąca dokumentacja analizy ryzyka dla ochrony DO - kwerenda wyników analizy ryzyka z ostatniego okresu z uwzględnieniem rekomendacji odnoszących się do środków technicznych i organizacyjnych, zapewniających ochronę DO. Zaktualizowane procedury w zakresie DO powinny uwzględniać ryzyko wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do DO, przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Warto uwzględnić również skutki dla ochrony DO, wymienione w mot. 75 preambuły, tj. ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, które może wynikać z przetwarzania DO prowadzącego do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych - w szczególności, jeżeli przetwarzanie może skutkować dyskryminacją, kradzieżą tożsamości.	*art. 24 i 32 RODO;* *mot. 26, 28, 29, 39, 74-78, 83 i 85 preambuły;* *Rozporządzenie KRI* *Standardy KZ*
		2. Czy prowadzona jest analiza ryzyka dla ochrony DO? Czy wyznaczono podmiot (osobę, stanowisko albo zespół) odpowiedzialny w tym zakresie?	[ocena wymogu]				
		3. Czy polityka ochrony DO jest oparta o analizę ryzyka? Czy uwzględnia wnioski oraz rekomendacje wynikające z analizy ryzyka dla ochrony DO z ostatniego okresu?	[ocena wymogu]				
		4. Czy zastosowano wskazane w rekomendacjach (IOD albo innego właściwego podmiotu) środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający zidentyfikowanemu ryzyku?	[ocena wymogu]				
VI.2 Ochrona danych w fazie projektowania oraz domyślna ochrona danych	[ocena obszaru]	1. Czy obowiązujące w jednostce pozostałe procedury, polityki wewnętrzne lub powtarzalne praktyki uwzględniają zasadę prywatności w fazie projektowania (privacy by design) oraz domyślnej ochrona danych (privacy by default)? W szczególności, czy ww. zasady znajdują odzwierciedlenie w procedurach jednostki odnoszących się do: - tworzenia prawa i regulacji wewnętrznych, - zarządzania projektami, - realizacji zamówień publicznych oraz - projektowania i modyfikacji systemów teleinformatycznych.	[ocena wymogu]			Informacja od ADO, IOD, Administratora Systemu Informacji (albo inny właściwy pracownik ds. IT). Wgląd w dokumentację z wykonanego przeglądu systemów (o ile taka została sporządzona). Uwaga: Każdy program, aplikacja lub system IT, wykorzystywany do przetwarzania DO, powinien mieć domyślne ustawienia przewidujące ochronę DO. Obowiązek zapewnienia domyślnej ochrony danych dotyczy ilości zbieranych danych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. Należy zobowiązywać wytwórców/dostawców aplikacji, usług i produktów, w ramach których przetwarzane są DO, by prawo do ochrony DO było uwzględniane już w fazie opracowywania i projektowania. Ponadto, ww. wytwórcy/dostawcy z należytym uwzględnieniem stanu wiedzy technicznej powinni zapewniać ADO i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązkach ochrony danych. Zwrotnie, zasada uwzględniania ochrony danych w fazie projektowania i zasada domyślnej ochrony danych powinna być uwzględniana w przetargach publicznych. Ponadto: 1. W ustawieniach początkowych systemów przetwarzających DO, jako domyślne jest ustawiona ochrona prywatności, a zmiana takiego ustawienia może następować jedynie na wyraźne żądanie użytkownika programu/systemu. 2. Domyślnie, czyli bez konieczności jakiejkolwiek aktywności osób, których dane dotyczą – i to w kluczowym dla użytkownika momencie przyłączenia się do danego systemu. 3. Domyślnie powinny być przetwarzane tylko te dane, które są niezbędne do osiągnięcia celu, dla którego zostały zebrane (minimalizacja danych).	*art. 25 i 28 RODO;* *mot. 78 preambuły.*
		2. Czy dokumentacja jednostki zawiera potwierdzenie faktu zobowiązania wytwórców/dostawców aplikacji, usług i produktów do stosowania wymogów RODO? Np. czy w konkretnych przypadkach zawierania umów z podwykonawcami przewidziano: - konsultacje albo uczestnictwo osób pełniących funkcje ADO albo IOD? - obowiązek każdorazowego, szczegółowego uzasadnienia konieczności rozwiązań skutkujących przetwarzaniem DO? - zasadę minimalizowania ilości i zakresu i okresu przetwarzania DO?	[ocena wymogu]				
VI.3 Identyfikacja istotnego ryzyka dla ochrony DO	[ocena obszaru]	Czy identyfikuje się operacje przetwarzania danych, dla których poziom ryzyka naruszenia praw lub wolności osób fizycznych oceniono, jako wysoki? Czy uwzględniono wyniki analizy ryzyka z ostatniego okresu?	[ocena wymogu]			Informacja od ADO i IOD. Należy zwrócić uwagę na charakter przetwarzanych danych (np. dane wrażliwe) oraz wyniki analizy ryzyka. Analiza ryzyka powinna odnosić się do wszystkich procesów wskazanych w rejestrze czynności przetwarzania.	*art. 35 RODO;* *mot. 84, 89-93 preambuły.*

	A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
VI.4	Ocena skutków przetwarzania dla ochrony DO	[ocena obszaru]	Czy dokonano oceny skutków dla ochrony danych: a) dla których poziom ryzyka naruszenia praw lub wolności osób fizycznych oceniono, jako wysoki? (art. 35 ust. 1 RODO) b) wskazanych przez PUODO w wykazie rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny? (art. 35 ust. 4 RODO) c) po stwierdzeniu takiej potrzeby w trakcie przeglądu, o którym mowa w art. 35 ust. 11 RODO? Czy w badanym okresie stwierdzono taką potrzebę? d) po zaleceniu jej przez IOD w toku monitorowania przetwarzania DO?	[ocena wymogu]			Informacja od ADO i IOD. Dokumentacja dotycząca analizy ryzyka oraz oceny skutków. Wykaz PUODO, o którym mowa w art. 35 ust. 4 i 5 RODO. - Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. poz. 827). Uwaga: zgodnie z wytycznymi dot. oceny skutków (str. 15) ocena ta powinna być dokumentowana. Ocena tych danych wymagana jest w szczególności w przypadku: a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną; b) przetwarzania na dużą skalę szczególnych kategorii DO, o których mowa w art. 9 ust. 1, lub DO dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10; lub c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.	*art. 35 RODO;* *wytyczne dot. oceny skutków.*
VI.5	Zakres oceny skutków przetwarzania dla ochrony DO	[ocena obszaru]	1. Czy ocena skutków zawiera następujące elementy: (art. 35 ust. 7 RODO) a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym (gdy ma to zastosowanie) prawnie uzasadnionych interesów realizowanych przez ADO; b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów; c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą; d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę DO i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą i innych osób, których sprawa dotyczy.	[ocena wymogu]			Weryfikacja opracowanej oceny skutków. Informacja od ADO i IOD. Uwaga: kryteria oceny, o których mowa w wytycznych dot. oceny skutków, tj. 1. Ewaluacja lub ocena (mot. 71 i 91 preambuły); 2. Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne lub podobne istotne skutki (art. 35 ust. 3 lit. a RODO); 3. Systematyczne monitorowanie (art. 35 ust. 3 lit. c RODO); 4. Dane wrażliwe (art. 9 RODO); 5. Dane przetwarzane na dużą skalę (mot. 91 preambuły); 6. Dokonano porównania lub połączenia procesów przetwarzania danych; 7. Dane dotyczące osób wymagających szczególnej opieki (mot. 75 preambuły); 8. Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych (art.35 ust. 1 i mot. 89 i 91 preambuły); 9. Transgraniczne przekazywanie danych poza Unię Europejską (mot. 116 preambuły); 10. Gdy przetwarzanie samo w sobie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystania z usługi lub umowy" (art. 22 i mot. 91 preambuły).	*art. 32 i 35 RODO* *wytyczne dot. oceny skutków.*
			2. Czy podczas dokonywania oceny skutków uwzględniono wszystkie kryteria oceny, o których mowa w wytycznych dot. oceny skutków?	[ocena wymogu]				
VI.6	Zapewnienie udziału IOD w ocenie skutków przetwarzania dla ochrony DO	[ocena obszaru]	1. Czy ocena skutków przetwarzania była konsultowana z IOD?	[ocena wymogu]			Informacja od IOD. Dokumentacja świadcząca o konsultacjach i monitorowaniu wykonania oceny skutków, w tym pisma i notatki wewnętrzne. Uwaga: z art. 39 ust. 1 lit. c wynika obowiązek IOD udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych zgodnie z art. 35 RODO. Przypadki, w których IOD nie zgadza się oceną ADO lub ADO nie zgadza się z zaleceniami IOD, powinny być odnotowane w formie pisemnej (w formie notatki lub protokołu rozbieżności).	*art. 35 ust. 2, art. 39 ust. 1 lit. c RODO;* *wytyczne dot. oceny skutków.*
			2. Czy IOD monitorował wykonanie oceny skutków przetwarzania?	[ocena wymogu]				
VI.7	Uprzednie konsultacje	[ocena obszaru]	Jeżeli ocena skutków przetwarzania lub rekomendacja IOD w zakresie tej oceny wskazały na wysokie ryzyko przetwarzania, a ADO nie zastosował środków w celu jego zminimalizowania, to czy przed rozpoczęciem przetwarzania dokonano konsultacji z PUODO?	[ocena wymogu]			Informacja od ADO i IOD oraz pismo ws. konsultacji (zgodnie z art. 36 ust. 3 RODO).	*art. 36 RODO;* *mot. 94-96 preambuły;* *wytyczne dot. oceny skutków*

	A. Obszar badania:	B. Ocena obszaru:	C. Przykłady zagadnień, pytań kontrolnych i wymogów:	D. Ocena spełniania wymogu:	E. Uzasadnienie oceny obszaru:	F. Uwagi i komentarze:	G. Wskazówki metodyczne:	H. Podstawa prawna i źródła:
VII. NARUSZENIE OCHRONY DANYCH OSOBOWYCH								
VII.1	Podmioty właściwe w zakresie postępowania z naruszeniami ochrony DO	[ocena obszaru]	Czy ADO wyznaczył osoby właściwe w zakresie zgłaszania PUODO naruszeń ochrony DO, które skutkują ryzykiem naruszenia praw lub wolności osób fizycznych?	[ocena wymogu]			Informacja od ADO i IOD. Analiza treści przedmiotowej procedury (w tym ewentualnego wzoru zgłoszenia). Rejestr naruszeń ochrony danych. Analiza dokumentacji określających zakresy zadań i odpowiedzialności np. opisy stanowisk pracy, zakresy zadań. Analiza dokumentacji w zakresie naruszeń bezpieczeństwa (np. podrównanie z rejestrem incydentów bezpieczeństwa i procedurami SZBI). Uwaga: Analizując procedury należy zwrócić uwagę na podmioty decydujące i sposób określenia czy naruszenie jest naruszeniem i czy podlega zgłoszeniu do organu nadzorczego (pożądany jest udział IOD w tym procesie). Np.: - powołano stały zespół, który rozpatruje indywidualne przypadki, - określono przykładowy katalog możliwych naruszeń/incydentów, które stanowią incydent podlegający zgłoszeniu. Procedury w zakresie zarządzania incydentami naruszenia ochrony DO (wszelkie odpowiednio wdrożone techniczne środki ochrony, w tym środki organizacyjne, które zapewniają bieżącą identyfikację naruszeń ochrony DO i pozwalają szybko poinformować organ nadzorczy i osobę, której dane dotyczą o naruszeniu).	*art. 33 i 34 RODO;* *mot. 85-88 preambuły*
VII.2	Procedura postępowania z naruszeniami ochrony DO	[ocena obszaru]	Czy opracowano procedurę zgłaszania i postępowania z naruszeniami ochrony DO, która w szczególności uwzględnia: a) definicję naruszenia wymagającego zgłoszenia do organu nadzorczego? b) obowiązek niezwłocznego zgłaszania przez ADO naruszeń (w ciągu 72 godzin)? c) obowiązek dokumentowania wszelkich naruszeń ochrony DO, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych? d) wzór zgłoszenia spełniający wymaga art. 33 RODO? e) role oraz odpowiedzialność wszystkich podmiotów zaangażowanych w proces postępowania z naruszeniami DO? f) niezwłoczne zawiadomienie osoby, której dane dotyczą (jeżeli ma to zastosowanie)? g) prawnie uzasadniony interes organów ścigania, jeżeli przedwczesne ujawnienie naruszenia mogłoby utrudnić badanie jego okoliczności? g) wzór ww. zawiadomienia zgodnie z art. 34 RODO?	[ocena wymogu]				
VII.3	Rejestr naruszeń ochrony DO	[ocena obszaru]	Czy jest prowadzony rejestr naruszeń ochrony DO, który dokumentuje w szczególności : - wszystkie przypadki zgłoszeń, w tym tych, które nie podlegają obowiązkowi przekazania do PUODO, - podmioty podejmujące decyzje w związku ze zgłoszeniem oraz - sposób postępowania z poszczególnymi zgłoszeniami?	[ocena wymogu]				
VII.4	Zawiadomienia o naruszeniu ochrony DO	[ocena obszaru]	Jeżeli stwierdzono istotne naruszenia ochrony DO, to czy dopełniono obowiązku zawiadomienia PUODO oraz osoby, której dane dotyczą?	[ocena wymogu]			Informacja od ADO i IOD. Dowody potwierdzające stosowne zawiadomienia (jeżeli były one konieczne). W przypadku znacznej liczby incydentów badanie można ograniczyć do próby zawiadomień.	*art. 33 i 34 RODO;* *mot. 85-88 preambuły*

OGÓLNA OCENA SPEŁNIANIA OBOWIĄZKÓW W ZAKRESIE DANYCH OSOBOWYCH

Sporządził:

(data i podpis)

Zatwierdził:

(data i podpis)